Security Work Group
http://www.nitc.state.ne.us/tp/workgroups/security/index.htm

Monday February 24, 2003
10:00 A.M. to Noon
NSOB 6Y – Lincoln, NE

Minutes

A. Participants

Steve	Cherep	HHSS
Cathy	Danahy	Secretary of State / Records Management
Dwayne	Dvorak	University of Nebraska
Steve	Henderson	IMServices
Jerry	Hielen	IMServices
Steve	Rathje	Dept of Natural Resources
Leona	Roach	University of Nebraska
Steve	Schafer	Nebraska CIO
Ron	Schrock	Military
Eric	Wieczorek	Military
Ron	Woerner	Department of Roads

A. Discuss Draft NITC Wireless Security Policy (Based on NIST SP 800-48)

Participants offered numerous suggestions, which will be reflected in a revised document. Specific changes will include:

- Some of the information in the Executive Summary is too detailed, too technical, and too lengthy;
- The National Institutes of Health has adopted a wireless policy, which could also be used as a model;
- Move the checklist to the appendix and put it into a table format, so that it can be used as a checklist;
- Who will have the responsibility to look for rogue wireless devices? Several tools exist, including one called "Solar Winds."
- Clarify roles and responsibilities, including who should be notified;
- Wireless LANs should follow any IMServices / DOC operational standards;
- Use "shall" instead of "should";
- Add a glossary (see NIH document).

B. State Network Security Issues

Steve Henderson presented a draft set of network security standards. The experience with the SQL Slammer incident underscored the need for operational standards pertaining to staying current with security patches, providing physical security and other measures. Operational standards like these are essential to protect other users on a shared network.

IMServices hopes to publish these within a few weeks and may submit them for consideration through the NITC process.

C. Discuss Remote Access Policy

Discussion included the following points:

- Agencies need guidance regarding home-based access to state networks and computer systems.
- As a general rule, employees should avoid remote access using public facilities, such as a public library or Internet café. These environments require additional security measures to be sure that one does not inadvertently leave data or information in the computer that someone else could then access.
- Web-browser and Internet connections, including e-mail over the Internet, should only be used for non-critical applications.
- Smart cards can be used to provide a higher level of secure access.
- The guidelines should address the use of remote access software such as PC Anywhere.
- What type of authentication is needed in what circumstances?
- How do we address the issues of authorization and authentication?
- Do we need a password policy?
- Should we require automatic logoff after a period of inactivity?
- What is the best way for connecting field offices? Should these connections be inside or outside the firewall?
- Should sustained dial-in connections be protected by a firewall?
- What advice should agencies provide to employees regarding ways of protecting their own PCs, which they may be using when gaining remote access to state networks and computer systems?

The Directory Services Project, which IMServices has been developing, will provide more options for authentication. We will ask for future updates.

The remote access policy should communicate risks and issues that an agency should address. They should not try to address all situations.

D. Security Awareness

Jerry Hielen gave a report on the MOAT Trial Survey. 242 users responded, out of 700 or 800 who took the training. Responses were generally favorable, although there were some negative evaluations. Jerry will check with several of the larger state agencies to assess potential interest and whether to pursue an enterprise licensing approach.

E. Update on Disaster Planning

No significant developments.

B. Next Meeting Dates

Monday March 31, 2003 at 10:00 A.M. NSOB 6Y

NIPC Products &Contact Information

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the NIPC web-site (http://www.nipc.gov), one can quickly access any of the following NIPC products:

- NIPC Advisories - Advisories address significant threat or incident information that suggests a change in readiness posture, protective options and/or response.
- NIPC Alerts - Alerts address major threat or incident information addressing imminent or in-progress attacks targeting specific national networks or critical infrastructures.
- NIPC Information Bulletins - Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.
- NIPC CyberNotes - CyberNotes is published to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.